LA SEGURIDAD EN LAS TRANSACCIONES EN EL COMERCIO ELECTRONICO

DIANA SALAS ACEVEDO

CORPORACION UNIVERSITARIA DE LA COSTA

FACULTAD DE DERECHO

BARRANQUILLA

2010

LA SEGURIDAD EN LAS TRANSACCIONES EN EL COMERCIO ELECTRONICO

DIANA SALAS ACEVEDO

Trabajo de grado presentado como requisito parcial para optar al título de Abogado

Asesor
Dra. Oscar Peña Cossio

CORPORACION UNIVERSITARIA DE LA COSTA

FACULTAD DE DERECHO

BARRANQUILLA
2010

NOTA DE ACEPTACION

_____

_____

_____

_____

Firma del Asesor

_____

Jurado

_____

Jurado

Barranquilla, Septiembre de 2010

TABLA DE CONTENIDO

Pág.

RESUMEN

En la actual era de la Globalización es muy difundido el uso de la Internet, por tanto es importante tener en cuenta que las transacciones que se realicen se hagan de manera segura, y sobre todo de acuerdo a la legislación vigente en Colombia en esta materia.

La presente investigación trata el tema de la seguridad en las transacciones electrónica en Colombia, de acuerdo al marco regulatorio colombiano, e internacional, en el cual se encuentra que no hay una homogeneidad, aunque se utilizan cada día técnicas más avanzadas por parte de los usuarios de Internet, la cual no se encuentra fortalecida por su sistema confiable para los clientes.

El objetivo principal de esta investigación fue la de determinar la seguridad en las transacciones electrónicas, debido a los continuos delitos que existen al respecto. Se utilizó el método de investigación descriptiva, en donde se hizo la descripción de todos los elementos que hacen parte del proceso de realización de las transacciones electrónicas a través de la Internet.

En conclusión, se puede decir que debe exigirse una normatividad acorde a los adelantos tecnológicos y de los nuevos sistemas de delitos que se cometen en la red.

PALABRAS CLAVES: Transacción, Seguridad, Internet, Decreto, Legislación, Ley, Contrato.

ABSTRACT

the current one it was of the Globalization it is very diffused the use of the Internet, therefore is important to keep in mind that the transactions that are carried out make in a sure way, and mainly according to the effective legislation in Colombia in this matter.

The present investigation treats the topic of the security in the transactions electronics in Colombia, according to the Colombian, and international regulatory mark, in which is found that there is not a homogeneity, although they are used every day more advanced techniques on the part of the users of Internet, which is not strengthened by its reliable system for the clients.

The main objective of this investigation was the one of determining the security in the electronic transactions, due to the continuous crimes that exist in this respect. The method of descriptive investigation was used where the description of all the elements was made that make part of the process of realization of the electronic transactions through the Internet. In conclusion, one can say that an in agreement normatividad should be demanded to the technological advances and of the new systems of crimes that are made in the net.

KEY WORDS: Transaction, Security, Internet, Ordinance, Legislation, Law, Contract.

INTRODUCCIÓN

El internet, como herramienta de comunicación alcanza un efecto integrador que desdobla fronteras geográficas y permite la interrelación de sus usuarios en tiempo real, en algunos casos, quizás en muchos, sin restricciones legales que permitan otorgar confianza en tales relaciones, lo que implica el acceso abusivo a información restringida, y el consecuente delinquir virtual.

Como inconveniente primordial en estas relaciones virtuales a través del internet, se concluye que no existe un marco regulatorio homogéneo estandarizado a nivel mundial que permita mitigar el impacto de los delincuentes virtuales que día a día utilizan herramientas tecnológicas más elaboradas y efectivas en términos de recolección de información privada de un usuario de un portal de internet o de una tienda en línea que no esté fortalecida por un sistema de seguridad confiable para sus clientes.

Dada esta situación los organismos de seguridad en la materia y entidades de carácter privado han planteado opciones de seguridad con la finalidad de permitir a todos aquellos navegantes virtuales y potenciales consumidores de un mercado abierto, y literalmente sin limitaciones de tiempo y espacio, una obligada estandarización global en aspecto comunes en todo tipo de negocio donde se

realizan transacciones e intercambio de bienes y servicios por cifras incalculables anualmente.

La evolución de todos estos negocios y tiendas en línea ha ido de la mano con un marco legal puntual para cada país, donde si bien se regulan elementos como estructura física de funcionamiento, límites de transacciones, requisitos mínimos de operatividad de los portales e informes o auditorias especializadas, el gran inconveniente afrontado es su ámbito de aplicación, pues es contradictorio el hecho que se expidan normas y leyes en cada nación cuando la esencia misma del internet es la conexión del mundo con el mundo, por ejemplo, un cliente en Japón interesado en hamacas colombianas, que debe cumplir obligaciones legales en cada país, algunas veces en contraposición, lo que se aleja de su intereses en términos de rentabilidad financiera.

Aspecto de validez al abordar este tema es que no puede perderse de vista el hecho, que lo técnicamente posible en materia de transacciones vía internet necesariamente esté ajustado a derecho, e igualmente tampoco es viable que la aplicación de la norma sea técnicamente posible con los recurso técnicos en nuestro país, así como en todos aquellos en vías de desarrollo, quienes no cuentan con un plataforma informática solida conllevando a una limitante sin solución a los comerciantes y compradores.

1. LA SEGURIDAD EN EL COMERCIO ELECTRÓNICO

La seguridad indica la posibilidad de realizar cierto tipo de transacciones de forma segura en la red. El fluir de información a través de múltiples canales informáticos supone un sinfín de riesgos. La situación actual de desarrollo, computacional y de redes de información, ha puesto de manifiesto la importancia de detectar, prevenir y detener las violaciones a la seguridad[1] informática.

Los usuarios deben conocer los peligros presentes en la red, en aras de tomar las medidas de seguridad pertinentes para proteger sus equipos de potenciales daños. Estas intromisiones pueden tener diversos objetivos desde volver inoperante un sistema operativo hasta el robo de información de diversas terminales de la empresa o de toda esta, estos efectos tiene por supuesto un alto impacto en términos jurídicos. La individualización de los atacantes es entonces necesaria por los medios jurídicos y electrónicos a disposición pero es más bien necesaria la implementación de mecanismo de seguridad preventiva.

1.1 INTRODUCCIÓN AL COMERCIO ELECTRÓNICO

Es necesario antes de abarcar aspectos del comercio electrónico entender, qué es el comercio. Que no es más que la acción o efecto de negociar, la

[1] La actual realidad de los sistemas computacionales, en cuanto a la seguridad se refiere, es preocupante, con más frecuencia se verá en los medios de comunicación noticias de ataques informáticos como el que reportó la sociedad Hispasec Sistemas - empresa de seguridad y tecnologías de la información -, que puede consultarse en la página web http://www.hispusec.com

necesidad de suplir necesidades, primarias o secundarias, lo que concluye en el intercambio de mercaderías; lo cual es en esencia un acto comercial, como definición jurídica encontramos que es la adquisición de bienes o servicios a título gratuito u oneroso con destino a venderlos o arrendarlos.

La mayoría de las actividades señaladas como actos de comercio, han estado sujetas a una restricción: la interacción física de las partes contratantes, lo que es el aspecto fundamental del negocio jurídico. La manifestación de las voluntades de las partes, es un aspecto fundamental en tales actos, que se expresaba a través de un documento físico "papel" donde la firma manuscrita daba fe de lo acordado. En la actualidad, esta definición está siendo revaluada, atendiendo las diferentes alternativas que ofrece el mercado, en particular, por el comercio electrónico.

Punto fundamental en materia de comercio electrónico, es su formación basada en la experiencia, situación que marca el destino del comercio. Como lo expresa el Dr. Madriñan de la Torre al enunciar lo siguiente:

> "Dondequiera que floreció la costumbre fueron desarrollándose, relativamente pronto usos mercantiles comunes, los cuales por concentración, pasaron con facilidad a ser derecho. Así surge desde un principio el derecho consuetudinario mercantil, que es donde encuentra justamente el comercio su norma especial, como derecho de contenido análogo." [2]

[2] MADRIÑAN DE LA TORRE, Ramón E. Principios de Derecho Comercial. Séptima Edición. Bogotá: Editorial Temis S.A. 1997. p 25 a 32.

Las actividades comerciales han presentado siempre la tendencia hacia la internacionalización del comercio, que no es más que el uso de prácticas comunes entre comerciantes nacionales y extranjeros.

La normatividad en materia de comercio electrónico, nace como respuesta a esas prácticas comunes, supliendo entonces, el vacío que dejaba el derecho civil; lo que lleva a entregar al comerciante el carácter de profesional por adelantar una actividad especializada y con normatividad propia.

Los computadores han mostrado un constante desarrollo desde sus comienzos. Bill Gates y Paul Allen fundaron MICROSOFT en 1975. La compañía se especializaba en ese entones en el diseño y fabricación de sistemas operativos, Un año más tarde, se lanzó al mercado el APPLE I, por uno de los ingenieros de Hewlett Packard, quien posteriormente seria el fundador de la empresa APPLE COMPUTER.

Se puede mencionar otro gran adelanto en materia de sistemas operativos que puso fin a la era de las máquinas de escribir, como son los procesadores de texto" que fueron lanzados al mercado, como son el WORDSTAR y el WORDPERFECT. Posteriormente hacia el año 1981 irrumpió en el mercado el computador personal de la IBM, así como la primera hoja de cálculo llamada LOTUS, para 1982 la empresa APPLE COMPUTERS revoluciono el mercado con el MACINTOSH, presentando como novedad un sistema operativo, que

presentaba iconos y ventanas controladas por un dispositivo externo al equipo que fue llamada ratón.

En el año 1981 se lanzo la red internacional WORD WIDE WEB(www) y desde entonces se viene desarrollando diversas plataformas de navegación como son el NETSCAPE, INTERNET EXPLORER, FIREFOX y muchos otros de menos popularidad.

La importancia de usar sistemas operativos radica en otorgar agilidad e integridad a plataformas de trabajo tecnológicos, otorgando interfaces amigables a los usuarios, pero aun ante los beneficios que otorgan los sistemas operativos, la inseguridad en las redes de información, genera desconfianza en los mismos, lo que ha llevado a la concientización de los empresarios en el desarrollo de mecanismos de seguridad en el uso masivo de sistemas de comunicación.

La necesidad de contención de los ataques ha obligado al diseño de herramientas especializadas que de una u otra forma han hecho lenta la evolución de las transacciones electrónicas, ya que existe una percepción de inseguridad y desconfianza en los usuarios.

Tal sentir de los usuarios debe ser disipado y por el contrario se requiere propagar todos los mecanismos de seguridad a su disposición, la gran dificultad es que no se conocen estos mecanismos. La internet es sin duda alguna la red de redes,

que permite la interrelación usuario –usuario en tiempo real, realizar transacciones comerciales, almacenar datos, celebración de contratos y actos mercantiles.

Es entonces el caso entrar a abordar la concepción de comercio electrónico;

En primer lugar es necesario manifestar que la Ley Modelo de la CNUDMI sobre Comercio Electrónico no definió la concepción de este sin embargo, fue utilizado como base de explicación para referirse al empleo de técnicas electrónicas modernas como el EDI[3] y el mail o correo electrónico, incluyéndose también mecanismos de comunicación menos avanzados como el télex, la telecopia y el fax.

Los potenciales compradores, se conectan a la red desde su PC, necesitando de un tercero proveedor del servicio de conexión a redes, a través de servidores[4]. Una vez conectados, a través de los buscadores acceden a la página web buscada, encontrando vendedores y compradores, procediendo entonces mediante el envió y recibo de mensajes de datos a concretar un negocio.

El potencial de los negocios electrónicos es cada día más valorado con un

[3] El EDI - Intercambio Electrónico de Datos: es toda aquella transmisión de mensaje de datos a través de medios telemáticos.

[4] Los servidores, como su nombre lo indica, se utilizan para dar servicios a las demás computadoras que se encuentran interconectadas entre sí. Un servidor puede tener servicios de archivos, de correo, de impresión, de páginas WEB, de programas, etc., todo en un mismo equipo o en diferentes servidores, dependiendo del volumen de usuarios. Las funciones principales del Servidor son: a) Centralizar y concentrar la información; b) Centralizar las aplicaciones (correo, archivos, Web, programas, etc.). c) Estandarizar la operación de la empresa.

crecimiento potencial de oferentes y compradores dispuestos a obtener grandes utilidades en la red con grandes intereses de posicionar sus compañías en este medio de negocios. Si bien existe un auge de los negocios en línea no se puede dejar de señalar que el impacto no ha sido el esperado dada la inseguridad latente en estos tipos de transacciones.

"En Colombia existen 6,7 millones de Internautas. El número de adeptos a la red Internet ha tenido una curva creciente en nuestro país, sin embargo, esta concentrada en las grandes ciudades" [5].

Muchos municipios no pueden acceder a un computador, por consiguiente este es el principal inconveniente que afrontan los colombianos para conectarse a la internet, es por eso que el programa COMPARTEL, desarrollado e implementado por el gobierno, pretende ofrecer computadores a aquellos lugares remotos menos favorecidos.

El comercio electrónico, podemos estudiarlo desde su diferentes enfoques

Comercio electrónico negocio a negocio: se intercambian bienes y servicios entre empresas a través de la red Internet.

Comercio electrónico de empresa a consumidor: este tipo de comercio de se

[5] Caracol radio publicación Mayo 4 de 2007, pg. 1

caracteriza porque la empresa a través de los navegadores existentes coloca sus productos a disposición de los consumidores

Comercio electrónico de consumidor a empresa: este comercio le permite a los consumidores acceder a los diferentes productos que se ofrecen en la red, que pueden llegar a ser adquiridos a través de mecanismos informáticos[6].

Comercio electrónico entre consumidores: es el utilizado por las bolsas de empleo quienes actúan como intermediarios laborales entre el oferente de mano de obra y la empresa usuaria.

La clasificación presentada nos muestra la importancia de la seguridad física y jurídica en una transacción comercial en la internet Sin embargo, cada negocio pude tener una regulación específica en Colombia, por lo que es de vital importancia que el legislador defina la jurisdicción aplicable a estas transacciones de acuerdo con los tratados internacionales suscritos, sean de derecho público o de derecho privado, definir inequívocamente a que jurisdicción corresponde conocer una eventual controversia, lo que en la actualidad no está plenamente definido.

[6] Al respecto puede verse por ejemplo el libro Fundamentos del Comercio Electrónico. Barcelona: Editorial Gedisa S.A. 2001

1.3 MARCO JURÍDICO DEL COMERCIO ELECTRÓNICO EN COLOMBIA

El marco jurídico del comercio electrónico en Colombia se circunscribe a la siguiente normatividad:

- Ley 527 de 1999;
- Decreto 1747 de 2000;
- Resolución 26930 de 2000;
- Jurisprudencia y Doctrina
- Y Conceptos de la Superintendencia de Industria y Comercio

La Ley 527 de 1999 resultado del estudio en temas de derecho mercantil internacional; redactada por una comisión que de la que formó parte tanto el sector público como el privado liderado por el Ministerio de Justicia, convocando otros Ministerios como el de Comercio Exterior y Transporte, quienes se dieron la tarea de regular todo lo referente al comercio electrónico y el manejo de los mensajes de datos en Colombia.

Su razón de ser obedeció a la necesidad de implementar en la normatividad del país, un régimen jurídico acorde con las nuevas tendencias en las comunicaciones y en el comercio, de tal manera que se establecieran herramientas jurídicas y técnicas, que dieran un fundamento sólido y seguro a las transacciones electrónicas al revestir de confiabilidad, seguridad y validez el

intercambio electrónico de informaciones.

Con la Ley 527 de 1999, nuestro país marcha de la mano con las modernas tendencias del derecho internacional privado, adoptando legislaciones que llenan los vacíos normativos de la nación, ya que a falta de regulación en la materia.

2. LA SEGURIDAD Y LOS RIESGOS

Cuando hacemos alusión a los riesgos, se piensa inmediatamente en un daño, El Dr. Sarmiento expone el significado etimológico del término riesgo de la siguiente manera:

> *Por riesgo se entiende la contingencia de un daño, o sea, la posibilidad de que al obra se produzca un daño, lo cual significa que el riesgo envuelve una noción de potencialidad referida esencialmente al daño, elemento éste que estructura todo el derecho de la responsabilidad y le otorga a la teoría que lleva su nombre un contenido esencialmente objetivo en el análisis de los hechos y las conductas que traen como consecuencia un perjuicio.*[7]

El riesgo bajo el esquema del daño, desestima la culpa de la responsabilidad civil, como claramente lo expresa el Dr. Sarmiento:

> *La idea de riesgo se presenta entonces sustitutiva de la idea de culpa como fundamento de la responsabilidad civil, lo cual implica el desconocimiento total del dogma milenario heredado del de echo romano, según el cual no hay responsabilidad sin culpa comprobada", en el que se basa toda la teoría tradicional de la responsabilidad y donde el elemento culpa se constituye en presupuesto de existencia de la obligación de indemnizar*[8]

Se debe señalar que en la teoría del riesgo, el daño connota el elemento forzoso para la generación de responsabilidad civil.

Conlleva la concepción del riesgo ineludiblemente, al estudio de los diferentes doctrinantes en la materia y jurisprudencia de nuestras cortes Para tal fin se seguirá, la exposición del Dr. Sarmiento quien ejemplifica cada una de las siguientes tesis:

---

[7] SARMIENTO. GARCIA, Manuel Guillermo. Responsabilidad Civil. Ediciones Universidad Externado de Colombia. 2002. P. 180 y 181.
[8] Ibid

Riesgo - Provecho: esta tesis cuantifica la obligación de resarcir, con fundamento en el daño causado, estableciendo una relación directamente proporcional entre el beneficio y el daño.

Riesgo - Creado: la responsabilidad, en esta tesis, recae en quien desarrolla una actividad que crea riesgos.

Riesgo - Profesional: la normatividad en Francia, consagró este tipo de riesgo como el fundamento indemnizatorio del accidente de trabajo.

2.1 ¿A QUÉ RIESGOS ESTÁ EXPUESTO AL CONECTARSE A LA RED INTERNET?

Para protegerse de un eventual ataque debemos conocer a que nos enfrentamos, razón por la cual, es de vital importancia conocer los riesgos a que estamos expuesto al realizar transacciones electrónicas y, presentar o usar las herramientas tecnológicas adecuadas para repeler tales ataques..

Al conectarse a través del Network[9] a Internet, se corren riesgos como los siguientes:

1. Se crean vías de acceso para los virus que se encuentran en la red.

[9] Sistema operativo utilizado para la interconexión de redes.

2. Si un virus penetra un sistema operativo puede afectar todos los archivos de las unidades de almacenamiento de información y programas en general, dañándolos y afectando su funcionamiento.
3. La información almacenada en el computador, queda expuesta y puede llegar a ser conocida, borrada o modificada.
4. Corporativamente un virus puede traer como consecuencias la perdida de millones de pesos, o la parálisis de actividades, inclusive pérdida de información reservada etc.

Las amenazas en materia digital pueden agruparse en dos categorías[10]:

A) Los ataques de red: se efectúan a través de la red Internet, provocan un lento desempeño en el sistema operativo de las computadoras de la empresa, afectan el correo electrónico y las redes internas.

B) infiltraciones: se dirigen al interior de los sistemas operativos, funcionan descifrando las contraseñas de los usuarios para acceder a los computadores, donde se podrá posteriormente entrar a cualquier sistema operativo o a los demás equipos que se encuentren conectados a la red.

[10] Las dos categorías que se mencionan son expuestas por Robert D. Austin y Crhristopher A.R. Darby en el artículo EL MITO DE LOS SISTEMAS DE IT SEGUROS. Harvard Business Review. Junio de 2003

2.2 ATAQUES TECNOLOGICOS

En primer lugar al más relevante de los atacantes, “el hacker” término del inglés hack, que significa recortar. Usualmente se cataloga al hacker como aquel aficionado que busca defectos de diseño en los programas, que le permitan entrar a los mismos y obtener información o sencillamente violar la seguridad de una empresa.

Se tiene que hacker es aquel aficionado a la informática que busca defectos los sistemas operativos. Para los conocidos la materia, la definición correcta sería: experto que puede conseguir de un sistema informático cosas que sus creadores no esperan. El término hacker nació de los programadores del Institute of Tecnology de Massachusetts (MIT), quienes se hacían llamar así mismos hackers, alardeando de su capacidad como programadores.

De los pioneros de las prácticas de pirateo informático podemos reseñar a Kevin Mitnik, quien escribió el libro “El arte de la decepción”, en el 2003. Fue perseguido por pirateo de software por la modificación de datos de varias compañías como son Motorola y Nokia.

2.2.1 Internos. Los ataques internos provienen de la misma compañía, es atribuido usualmente como resultado de factores organizacionales como la inestabilidad laboral, ya que los empleados al no tener sentido de pertenencia recurren a

prácticas desleales y encuentran en la venta de información confidencial de la empresa una forma de lucro.

Estos tipos de atacantes son difíciles de prevenir y se depende exclusivamente de la lealtad y confianza entre el empleador y el trabajador

2.2.2 Externos. Suelen ser los atacantes más peligrosos pero son menos frecuentes, su prevención depende en su totalidad de los sistemas de seguridad con que cuente la empresa y sus aplicativos en las transacciones comerciales y manejo interno de la informacion.

Los atacantes pueden ser:

A) Los hackers: De Origen inglés, ampliamente conocidos a nivel mundial, su habilidad se centra en el ingreso ilegal a sistemas de información su denominación es inglesa y su nombre se generalizó a nivel mundial, la intención de estos personajes es demostrar su habilidad ingresando a sistemas y programas de forma ilegal, alterándolos y dañándolos.

B) Los: vándalos: Son atacantes que persiguen crear el caos, la histeria colectiva accediendo de forma abusiva a sistemas de información.

2.3 CLASES DE ATAQUE

Podemos definir como clases de ataque todos aquellos instrumentos utilizados para accesar sistemas de información modificándolos, o borrándolos esos ataques externos pueden ser;

2.3.1 Los virus. Los virus son programas que se inician o activan cuando se ejecuta un archivo, tiene la extensión .exe, afecta exclusivamente los ejecutables de los programas instalados en el PC, pueden auto clonarse con la finalidad de generar expansión, los correos electrónicos son la fuente usual de virus.

2.3.2 Gusanos. Fueron creados para infiltrarse en los procesadores de texto y destruir paulatinamente la información, no poseen capacidad de clonarse, debido a esto pueden ser fácilmente eliminados del sistema

2.3.3 Los caballos de Troya. Estos programas se encuentran escondidos dentro de otros programas o archivos, y su finalidad es hacer que un programa actúe de forma diferente a la prevista introduciendo a este una serie de rutinas específicas.

2.3.4 bomba de reloj. Muy similares a los caballos de Troya, diferenciados por que estos tiene el ataque programado a un tiempo específico o la ejecución de un programa específico.

2.3.5 La introducción de datos falsos. Esta forma de ataque externo consiste en modificar o usar datos del sistema operativo sea de entrada o de salida, produciendo errores y así aprovechar para sustraer información de la empresa.

2.3.6 Las vías de ataque. La efectividad en el ataque radica en la adecuada vía de acceso, lo que encuentran los hacker chequeando puntos álgidos de programación, regularmente identifican tales puntos débiles y vulnerables en un network y de esa forma entran a sistemas de información

La habilidad de poder violentar un sistema de seguridad informático es esgrimido siempre por el atacante como muestra de su conocimiento informático y la implementación de nuevos sistemas de seguridad se convierte en la meta del hacker para mostrar sus capacidades.

La forma más conocida de vías de ataque es:

2.3.7 Software Bugs. La misión del software bug es atacar la estructura de los programas y permitir el ingreso de hacker a un sistema informático, siempre se desarrollan para crear varias vías de acceso para el ataque.

2.4 CLASES DE SEGURIDAD

Encontramos básicamente dos mecanismos desarrollados a nivel de seguridad en

el comercio electrónico, herramientas de seguridad utilizada para adelantar el comercio en internet, los mecanismos desarrollados y de mayor importancia son:

a) Secure Electronic Transactions: Esta es la herramienta más usada en términos de seguridad en el comercio electrónico, popularizada por Visa y MasterdCard. Proporciona seguridad en las comunicaciones a través de Internet entre el emisor de una tarjeta de crédito, su titular, y la entidad financiera.

Las empresas emisoras de tarjetas de crédito, han creado una comunidad con la finalidad de adelantar un comercio electrónico de forma segura. SET que no es más que un conjunto de especificaciones que proporciona una canal seguro para poder realizar transacciones electrónicas. Este usa todas las herramientas de seguridad disponibles para asegurar las transacciones. Actualmente, casi todas la entidades crediticias internacionales están implementando este protocolo para garantizar la seguridad de sus usuarios en la red, en la actualidad en nuestro país está siendo usado el protocolo SSL.

b) Secure Sockets Layer (SSL): Es un sistema estandarizado por Netscape, este utiliza tecnología de para encriptar las comunicaciones entre el usuario y los servidores.

Está claro que el protocolo SET es el sistema ajustado para las instituciones financieras, por ser su servicio de carácter público, aunque como se mencionó, el

protocolo usado en nuestro país es el SSL, que endilga los manejos fraudulentos o hurtos por perdidas de claves y clonación de tarjetas a los tarjetahabientes. El titular del producto es responsable por el manejo de la información confidencial que le ofrezca la entidad financiera en el buen uso de sus servicios financieros. En nuestro país la responsabilidad de este tipo situaciones no se ha definido, por lo que las Defensorías del Cliente Financiero[11], estaría obligado a imponer las condiciones mínimas de seguridad con que deben contar las entidades en virtud de su manejo de dineros de terceros.

2.4.1 Seguridad en el Host y en el Network. Se distinguen dos modelos básicos de protección informática que pueden utilizarse separada o conjuntamente: Seguridad en el host y Seguridad en el network.

La seguridad en el host es la forma más común, se aplica a cada computador y tiene gran acogida en empresas pequeñas. Este sistema utiliza tres programas de seguridad -Firewalls individuales: Controlan la remisión y recepción de información. Sandbox: es un zona segura no conectada a la red cuya función es probar los programas antes de su ejecución en nuestro PC. Scanning: se encarga de comprobar que los programas y los discos duros no tengan virus.

La segunda por su parte controla desde el network el acceso a los host, para lo

[11] Las Defensorías del Cliente se establecieron por virtud de la Ley 795 de 2003 y su reglamentación está dada por el Decreto 690 de 2003.

cual utiliza diversos mecanismos entre los cuales pueden mencionarse: -Firewalls: A través de programas de software y hardware se crea un sistema de puertas que controlan la entrada y salida al network.

Hay tres tipos básicos de firewalls:

Filtro de paquetes: Escanea el tránsito de la red en la zona de paquetes. Cuando se envía un paquete por Internet, este es examinado detenidamente, y se le permite el paso o se rechaza.

Claves: Es un sistema de claves que sólo son conocidas por las personas autorizadas para ello, lo que genera seguridad al acceso de programas privados y al network en general.

Servidor proxy: Sistema de bloqueo para lograr controlar la entrada de los virus al servir del intermediario entre las páginas web a las que entra el usuario y las operaciones que se aceptan luego de revisada la información tanto la que ese envía como la que se recibe.

2.5 COMERCIO SEGURO

Adicionalmente se debe tener en cuenta al ingresar a un sitio seguro, la

confidencialidad, la integridad, la autenticación y no rechazo de los mensaje de datos que se envíen, esto es gran relevancia pues allí se centra la confiabilidad de los servidores en internet, por lo que esos sitios web estarían en capacidad de mantener la información privada, integra, una adecuada autenticación de usuarios y el no rechazo de mensajes de datos

Para realizar una transacción segura en internet deben verificarse unos elementos indispensables como son:

Confidencialidad de las transacciones electrónicas: De tal forma que solo los intervinientes en la transacción puedan acceder a la información o datos que esta conlleva y solo ellos puedan modificarla.

Integración de firmas digitales: Consiste en el uso de las firmas digitales de tal suerte que la identificación de un usuario sea inequívoca, para que su contenido no pueda ser adulterado por otros usuarios.

EL uso de certificaciones digitales para la comprobación de la autenticidad del medio de pago, de los titulares de las transacciones y muchos otros aspecto relevantes a esta. La garantía de la identidad de los intervinientes en una transacción en internet debe estar avalada por un tercero en capacidad de expedir certificación digital (un notario electrónico.)

Otro herramienta de seguridad importante y que debe ser objete de estudio es la infraestructura de clave pública (PKI, Public Key Infraesctructure), que tiene como base de trabajo la encriptación, para hacer indescifrables mensajes de datos y alcanzar el mismo nivel de seguridad que se podría encontrar en las transacciones cara a cara.

2.6 DELITO INFORMÁTICO

La Ley 1273 de 2009 estructuro nuevos tipos penales respecto a delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.

El 5 de enero de 2009, se promulgó la Ley 1273 "Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "De la Protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"[12].

Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de información personal, por lo que es de gran importancia que las empresas se cubran jurídicamente para evitar incurrir en alguno de estos tipos penales.

[12] Ley 1273 del 5 de Enero de 2009 del Congreso de la República de Colombia. Diario Oficial No.47223 de 5 de enero de 2009.

Es perfectamente comprensible que los avances en la tecnología y el uso de la misma para apropiarse de forma ilícita del dinero de terceros a través de duplicación de tarjetas de crédito, alteración de los sistemas de computación para recibir servicios y depósitos electrónicas de fondos mediante el uso de programas y manipulación de cajeros automáticos, entre otras, son conductas cada vez más usuales en todas partes del mundo. Según la Revista Cara y Sello, durante el 2007 en Colombia las empresas perdieron más de 7.9 billones de pesos a raíz de delitos informáticos.

He aquí importancia de la ley, que adiciona al Código Penal colombiano el Título denominado "De la Protección de la información y de los datos" que dividida en dos capítulos, “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” y “De los atentados informáticos y otras infracciones”.

El primer capítulo modifica los siguientes artículos:

> *Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.*
>
> *Artículo 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios*

mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269E: USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269F: VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes[13]*.*

Es importante aclarar que la Ley 1266 de 2008 definió el término dato personal como “cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica”. El artículo obliga a las empresas un especial cuidado en el manejo de los

[13] Ibid. Titulo VII BIS. “De la protección de la información y de los datos. Ley 1273 de 2009.

datos personales de sus empleados, toda vez que la ley encarga a quien "sustraiga" e "intercepte" dichos datos a pedir autorización al titular de los mismos.

> *"Artículo 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave"*[14].

Esta misma sanción será impuesta al que modifique el sistema de nombres de dominio, de tal manera que haga entrar al usuario a una dirección web diferente a la que pretende o cree acceder, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena indicada en los incisos anteriores tendrá como agravación de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas durante la comisión del delito.

Es importante señalar que este artículo tipifica lo que se conoce como "pishing", modalidad de estafa que usualmente utiliza como medio el correo electrónico pero que cada vez con más frecuencia utilizan otros medios de propagación como por ejemplo la mensajería instantánea o las redes sociales. Según la Unidad de

[14] Ibid, p.13

Delitos Informáticos de la Policía Judicial (Dijín) con esta modalidad se robaron más de 4.200 millones de pesos en el año 2007.

Un punto importante a considerar es que el artículo 269H adiciona circunstancias de agravación punitiva de los tipos penales descritos anteriormente el aumento de la pena de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones
3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para si o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.
8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Es importante recalcar que estos tipos penales obligan a empresas y a personas naturales a volcar una especial atención al tratamiento de equipos informáticos así como al tratamiento de los datos personales más teniendo en cuenta la circunstancia de agravación del inciso 3 del artículo 269H que señala “por quien tuviere un vínculo contractual con el poseedor de la información”.

Se hace entonces necesario incluir unas condiciones en las contrataciones, a empleados y contratistas, para evitar incurrir en la tipificación penal.

Por su parte, el capítulo segundo establece:

> *Artículo 269I: HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 del Código Penal, es decir, penas de prisión de tres (3) a ocho (8) años.*
>
> *Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes.*
>
> *La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa*[15]*.*

[15] Ibid. p.13

Cuando la conducta descrita en los incisos anteriores fuera de cuantía superior a 200 salarios mínimos legales mensuales, la sanción se incrementará en un 50 % o sea la mitad.

La Ley 1273 adiciona una circunstancia de mayor punibilidad en el artículo 58 del Código Penal al hecho de realizar las conductas punibles utilizando medios informáticos[16].

Igualmente la Ley 1273 dio un paso importante en la lucha contra los delitos informáticos en Colombia, por lo que es necesario prepararse legalmente para enfrentar los retos planteados.

La nueva ley presenta la necesidad para los empleadores de crear herramientas adecuadas para proteger sus activos más valiosos como lo es la información.

Las compañías deben aprovechar la expedición de esta norma para adecuar sus contratos, señalar deberes y sanciones a sus empleados en reglamentos internos de trabajo, presentar acuerdos de confidencialidad con los mismos y crear puestos de trabajo que velen por el cumplimiento de la norma en comento, atendiendo a las sanciones a las que pueden verse expuestas.

Por otro lado, se hace imperativa la regulación de los aspectos de las modernas modalidades de trabajo como es el trabajo online, los call centers y muchos otros, que exigen un nivel alto de supervisión respecto al flujo de información delos

[16] http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia

clientes, igualmente, resulta conveniente realizar capacitaciones y seminarios al interior de las organizaciones con el fin de que los trabajadores sean conscientes del nuevo rol que desempeñan en el nuevo mundo de la informática y del internet en las compañías del nuevo milenio.

Teniendo en cuenta lo anterior es relevante analizar todos aquellos perjuicios económicos a los que se pueden enfrentar las compañías por el uso inadecuado de la información por parte de sus trabajadores y demás personas relacionadas con la empresa indistintamente al tipo de contratación que tengan.

Más allá de ese relevante factor, con esta ley se obtiene una herramienta importante para poner en conocimiento los hechos delictivos que se puedan observar, esto es una modificación importante si se tiene en cuenta que anteriormente las empresas no denunciaban dichos hechos no sólo para evitar daños en su reputación sino por no tener herramientas especiales.

3. LA EFECTIVIDAD DE LOS MENSAJES DE DATOS COMO MEDIO DE PRUEBA.

Las nuevas tecnologías de la comunicación, a pesar de sus grandes y evidentes ventajas, no tenían el aval como medio de prueba, lo cual hacía que su uso en negocios y contratos fuera muy limitado. Como solución, el legislador se dio a la tarea de regular y dotar de fuerza jurídica y probatoria este tipo de medios. Fue así como se gestó la teoría del equivalente funcional, que no es otra cosa, que dotar al documento electrónico de las mismas características que posee el documento físico.

En este orden de ideas, es importante mencionar, cuales son las características del documento físico, que pueden sintetizarse de la siguiente manera:

I. Legible por todos

II. Inalterabilidad a lo largo del tiempo

III. Permitir su reproducción para que cada una de las partes tuviera un ejemplar del mismo.

IV. Autenticación de los datos consignados mediante una firma

V. Presentación formal y aceptable de un escrito ante las autoridades públicas y los Tribunales

El Artículo 251 del Código de Procedimiento Civil define la noción de documento en los siguientes términos:

> *ARTÍCULO 251. DISTINTAS CLASES DE DOCUMENTOS. Son documentos los escritos, impresos, planos, dibujos, cuadros, fotografías, cintas cinematográficas, discos, grabaciones magnetofónicas, radiografías, talones, contraseñas, cupones, etiquetas, sellos y, en general, todo objeto mueble que tenga carácter representativo o declarativo, y las inscripciones en lápidas, monumentos, edificios o similares.*
> *Los documentos son públicos o privados.*
>
> *Documento público es el otorgado por funcionario público en ejercicio de su cargo o con su intervención. Cuando consiste en un escrito autorizado o suscrito por el respectivo funcionario, es instrumento público; cuando es otorgado por un notario o quien haga sus veces y ha sido incorporado en el respectivo protocolo, se denomina escritura pública.*[17]

¿Qué diferencia existe entre documento público y documento privado?; para tal efecto y, con el fin de entender dicha diferencia, se pueden identificar los siguientes puntos que explican la diferencia de la siguiente manera:

a) Es la publicidad la que distingue a los documentos, en públicos y Privados.

b) Tanto los documentos públicos como los privados pueden estar contenidos en escritos, o en otras formas gráficas.

c) El documento público puede utilizar la forma gráfica u otra diferente, pero

[17] TORRADO, Helí Abel. Código de Procedimiento Civil de la República de Colombia. DEd. Sergio Arboleda. 3ª Ed. Noviembre de 2004. p. 256

cuando es escrito y autorizado por el respectivo funcionario, se denomina instrumento público. Este es, pues, una especie del documento público.

d) El documento público, que a la vez sea instrumento público, cuando es otorgado por un Notario e incorporado en el protocolo, toma la denominación de escritura pública. Esta es, pues, una especie del instrumento público, y una subespecie del documento público.

e) Los demás son documentos privados.

Es importante, aclarar y diferenciar, como lo expresa FRAMARINO[18], la diferencia entre publicidad y autenticidad: la publicidad, pretende dar fe ante todos de la autenticidad: el funcionario público da fe ante las partes contratantes y, con efectos erga omnes, que las firmas de los intervinientes, que aparecen suscritas, son las de los autores que se enuncian en el documento. Por eso resulta correcto decir que, documento público es el que hace fe pública de su autenticidad.

El mensaje de datos cumple las características del documento escrito y en algunos casos, inclusive, supera las expectativas que en un principio se tuvo de él, aún más, el mensaje de datos, por su especial condición técnica es más

[18] FRAMARINO DEI MALATESTA, Incola. Lógica de las pruebas. Bogotá: 1964. p. 11. Citado por RODRÍGUEZ. Ibid. p. 231.

seguro que el documento consignado en un papel. Así, lo expresó la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. Otro aspecto de trascendental importancia en la búsqueda de este objetivo, es la verificación de la autenticidad, la conservación y la consulta, como requisitos que debe cumplir el mensaje de datos para lograr su cometido.

3.1 EL DOCUMENTO ESCRITO

La Ley 527 de 1999 señala en su articulado que sí el documento electrónico es fácilmente accesible para su posterior consulta, se debe asegurar su forma escrita.

En el contrato de seguro celebrado a través de la red, el perfeccionamiento, se daría de bajo la siguiente formalidad:

1. El tomador del seguro ingresa a la página web de la aseguradora;
2. Ubica el seguro que necesita tomar
3. Envía sus datos personales de acuerdo con el cuestionario que para tal efecto diseñe la aseguradora;
4. La aseguradora realiza una investigación de los datos Personales del solicitante. Para llevar a cabo dicha investigación puede valerse de la Autoridad de Certificación, o verificar con la Entidad de Certificación, que cumpla las funciones de Autoridad de Certificación,

sí el solicitante se encuentra registrado en la base de datos de la entidad. Si se encuentra registrada en la AC, se procede a la expedición en línea del seguro, de lo contrario será necesaria la corroboración de los datos personales a través de medios idóneos que garanticen o certifiquen la veracidad de los datos.

5. Después de realizado el estudio del tomador y del estado del riesgo, la aseguradora manifiesta su aceptación y da vía libre a la expedición del seguro. A partir de este momento el contrato existe, y la prueba de este, o sea la póliza, debe ser entregada por la aseguradora dentro de los quince días siguientes al perfeccionamiento del contrato, y una vez efectuada la entrega comienza el término para pagar la prima del seguro. La entrega de la póliza es un paso que puede obviarse si se contrata a través de la red; una vez perfeccionado el contrato el tomador podrá imprimir la póliza y tener la prueba de la existencia del contrato.

El aspecto de mayor relevancia en estos eventos es que se verifique la seguridad que el contrato no será ni modificado ni alterado en su forma electrónica o física, esto solo se logra cumpliendo los requerimientos de ley respecto a las herramientas de confiabilidad implementadas. Por lo que se tiene que aún si el acuerdo de voluntades se dio en un ambiente inseguro, sin el respaldo escrito, no se pierde el valor probatorio en sí mismo del mensaje de datos, lo que se ve afectada es su confiabilidad entorpeciendo el comercio financiero.

En virtud de la Ley 527 de 1999, si celebramos a través de la Internet un contrato, que exija por imperio de la ley la formalidad escrita, es necesario, que dicho documento pueda traerse a físico o que se pueda acceder para su posterior consulta, su valor probatorio dependerá del entorno de seguridad que rodeó el acuerdo de voluntades.

Todos los mensaje de datos obtienen su valor probatorio en la misma ley, independientemente del tipo de seguridad que lo avale. Por lo que su presencia como prueba en un juicio debe ser , obedecer a un enfoque respecto a la idoneidad del negocio jurídico celebrado, lo cual es directamente proporcional a la seguridad utilizada.

Se tiene entonces que si el contrato está protegido por una firma digital, es incluso, mucho más confiable que un documento físico, ya que está de por medio y como garante del acto o negocio, una Entidad que responde civilmente por la autenticidad del documento.

La promesa de compra - venta de inmueble, o el contrato de seguro entre otros, podrán realizarse por vías electrónicas siempre y cuando el sistema empleado-software-, permita la reproducción o posterior consulta del documento y garantice la idoneidad del documento. Los documentos electrónicos son documentos que sirven como medio de prueba en cualquier proceso judicial y, tendrán el más alto valor probatorio, si está de por medio una Entidad de Certificación, o,

mecanismos idóneos de seguridad que garanticen la integridad del documento.

3.2 LA AUTENTICIDAD DE LOS DOCUMENTOS

El artículo séptimo de la Ley 527 de 1999, refiere el tema de la autenticación del mensaje de datos. La autenticidad es la verdad de la indicación del autor, es decir, la correspondencia entre el documento y su autor. La autenticidad es el elemento más relevante del documento para su eficacia probatoria.

La autenticidad del mensaje de datos, de acuerdo con el artículo séptimo de la Ley 527de 1999, se da en aquellos casos en donde para la creación del mensaje de datos se utilizó un método confiable y a su vez dicho método permite identificar al iniciador del mensaje. Un sistema confiable es aquel que satisface los estándares establecidos por la Superintendencia de Industria y Comercio (Artículo 2º Decreto 1747 de 2000). El Superintendente de Industria y Comercio, en uso de sus facultades legales, en especial las conferidas en los artículos 29, 34, 41 y 42 de la Ley 527 de 1999 y los Decretos 2153 de 1992, 2269 de 1993 y 1747 de 2000, expidió la Resolución 26930, que en su artículo 20 nos habla de un "Sistema Confiable"

3.3 CONSULTA Y CONSERVACIÓN

Nuestra legislación ha definido los parámetros que deben observarse:

Encontramos entonces que en el artículo octavo (8º) de la Ley 527 de 1999, vislumbra la posibilidad de conservar un mensaje de datos en su formato original, existiría pues una garantía para que el mensaje de datos no sea alterado y pueda ser presentado - exhibido - en el tiempo que se requiera.

La garantía, no es más que la creación del mensaje de datos a través de una herramienta confiable y su almacenamiento en un sistema que garantice la no - alteración y, su posterior consulta y exhibición a la autoridad que lo requiera. El artículo 12 de la Ley 527 de 1999 establece las condiciones para la "Conservación de los mensajes de datos y documentos" permitiendo que la conservación se pueda hacer directamente o través de terceros siempre y cuando se cumplan con las exigencias del artículo 12 en mención.

En los casos en que los mensajes de datos sean creados a través de entidades de Certificación, el Artículo 38 de la Ley 527 de 1999 dispone que los registros de certificados deben ser guardados o archivados por el término exigido en la ley que regule el acto o negocio jurídico en particular.

Las Entidades de Certificación abierta tienen dos deberes a saber, una es el almacenamiento de datos y otra garantizar su conservación. Artículo 13 Decreto 1747 de 2000:

> *Garantizar el acceso permanente y eficiente de los suscriptores y de terceros al repositorio de la entidad y Conservar la documentación que respalda los certificados emitidos, por el término previsto en la ley para los papeles de los comerciantes y tomar las medidas necesarias para garantizar la integridad y la confidencialidad que le sean propias*[19].

El mensaje de datos al momento de su creación, debe permitir su posterior consulta y garantizar su conservación en el tiempo. Si se cumplen estas exigencias el mensaje de datos tendrá valor probatorio. Ahora bien, cuando el mensaje de datos es creado en un entorno confiable, esto es, con la intervención de un tercero de confianza - Entidades de Certificación - se garantiza: la inalterabilidad del mensaje de datos a lo largo del tiempo y, su posterior consulta, con un elemento adicional muy importante, perfectas condiciones de calidad aún con el transcurso del tiempo. Es muy importante que el juzgador tenga en cuenta que la eficacia probatoria del mensaje de datos depende directamente de su confiabilidad, es decir, la garantía de inalterabilidad y no repudio.

A través de los diferentes mecanismos de seguridad, y en especial el ofrecido por las Entidades de Certificación, se garantiza en forma integra todas y cada una de las características del documento escrito y se genera más seguridad por el contexto tecnológico.

Los paquetes de datos pueden asegurar la misma confiabilidad que cualquier

[19] Decreto 1747 de Septiembre 11 de 2000. Ministerio de Desarrollo Económico. Reglamenta La ley 527 de 1999. Diario oficial 44.160. Ministerio de Desarrollo Económico.

documento escrito, logrando la misma finalidad, lo que jurídicamente se traduce en que el documento electrónico al igual que el documento físico son medios de prueba, en si mismos considerados.

3.4 EL DOCUMENTO ELECTRÓNICO

Una vez lograda la eficacia probatoria de los paquetes de datos podemos definir el documento electrónico de la siguiente forma:

"Es un objeto físico dirigido a conservar y transmitir informaciones mediante mensajes en lenguaje natural, realizado con la intermediación de funciones electrónica"[20]

Ante esta definición y para no generar confusiones frente a la noción de lo físico" en el documento electrónico, puede afirmarse que es un objeto intangible que puede de transformarse a físico, y percibirle por los sentidos, que contiene información que puede ser jurídicamente válida y representa la voluntad del creador o creadores; y que es construido con la intermediación de herramientas electrónicas que pueden garantizar su confiabilidad.

Ahora bien, una vez expuesta la posición de la legislación y la doctrina

[20] Tribunal Supremo de Justicia de la República de Venezuela. Disponible en http://zulia.tsj.gov.ve/decisiones/2008/enero/516-15-32439-044.html. Barranquilla, Agosto 23 de 2010. 4:30 p.m.

colombiana respecto al mensaje de datos como medio de prueba, es importante conocer la posición de la Jurisprudencia como fuente de derecho en nuestra legislación.

3.5 JURISPRUDENCIA

La Corte Constitucional atendiendo la demanda de inconstitucionalidad contra los Artículos 10, 11, 12, 13, 14, 15, 27, 28, 29, 30, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45 de la Ley 527 de 2001, por estimar que violan los artículos 131 152 y 153 de la Constitución Política, tuvo la oportunidad de pronunciarse con respecto a la Ley 527 de 1999 y en particular frente a los mensajes de datos y su capacidad probatoria.

Se analizará esta providencia que es la de más alcance en la materia hasta el momento proferida por la Corte Constitucional en materia de comercio electrónico

Sentencia C-662 de Junio 08 de 2000;

Con respecto a los Artículos 152 y 153 de la Carta Magna, el actor considera que no se salvaguardo la reserva de ley ni los trámites contemplado en el Artículo 153. De la Constitución Nacional Los Artículos demandados son: 9°, 10, 11, 12, 13, 14, 15 y 28 de la Ley 527 de 1999.

Según el actor, atacado cuestiona, modificar y adiciona el Código de Procedimiento Civil, lo que en su concepto equivale a administrar justicia al atribuir a los mensajes de datos fuerza probatoria per se.

Debe tenerse en cuenta la posición de nuestra Corte Constitucional con relación a la importancia de la incorporación de una Ley de referencia respecto al Comercio Electrónico al ordenamiento jurídico de nuestra nación, que como manifiesta esa misma corporación, expande nuestras fronteras comerciales.

En la parte considerativa, el Alto Tribunal, comienza su análisis describiendo las características del mensaje de datos en los siguientes términos:

1. Es una prueba de la existencia y naturaleza de la voluntad de las partes de comprometerse.
2. La segunda característica es que dicho documento es legible y puede ser presentado ante las autoridades públicas y los tribunales.
3. Facilita la revisión y posterior auditoria para los fines contables, impositivos y reglamentarios.
4. Admite su almacenamiento e inalterabilidad en el tiempo. Efectivamente el mensaje de datos al encontrarse en un sistema electrónico puede ser almacenado por largos períodos de tiempo, lo que no garantiza que no pueda ser alterado, de hecho, está expuesto a un sin número de riesgos, que van desde la alteración, modificación e interceptación del

mensaje, hasta su destrucción, razón por la cual no puede decirse que un mensaje de datos como tal es inalterable. Para que sea difícilmente alterable se requiere que esté protegido, por ejemplo, por una Entidad de Certificación o con claves y códigos complejos, sin embargo, aún así está expuesto.

5. Afirma derechos y obligaciones jurídicas entre los intervinientes y es ulterior para su posterior consulta, es decir que la información en forma de datos computarizados es susceptible de leerse e interpretarse.

Es importante tener en cuenta que los mensajes de datos no siempre conllevan en sí mismos un contenido de carácter jurídico; un e-mail es un mensaje de datos y en la mayoría de los casos no incorpora o no tiene como fin establecer una relación de tipo jurídico, muchas veces son cartas de amor, fotos o anécdotas de viajes etc.; un fax es un mensaje de datos y generalmente tiene una función informativa, generalmente no busca generar derechos y obligaciones.

El actor considera que todo aspecto sustantivo o procesal relacionado con la administración de justicia está reservado al ámbito de la ley estatutaria de acuerdo con el Artículo 152 constitucional. Al respecto, la Corte considera que el demandante parte de una premisa equivocada, "como quiera que la accionante parte de un erróneo entendimiento acerca del ámbito material que constituye la reserva de la ley estatutaria sobre la administración de

justicia".

En conclusión la reserva de la ley estatutaria no significa que cualquier asunto y regulación relacionada con los temas previstos en el Artículo 152 requieran el trámite especial ahí previsto.

Con respecto a la condición del mensaje de datos, como medio probatorio, la Corte expresó:

> *[...] al hacer referencia a la definición de documentos del Código de Procedimiento Civil, le otorga al mensaje de datos la calidad de prueba, permitiendo coordinar el sistema telemático con el sistema manual o documentario, encontrándose en igualdad de condiciones en un litigio o discusión jurídica, teniendo en cuenta para su valoración algunos criterios como: confiabilidad, integridad de la información e identificación del autor*[21].

De otra parte, la Corte encuentra que el Artículo 4º del Decreto 266 del 2000, expedido por el Presidente de la República en ejercicio de las facultades extraordinarias conferidas por el Numeral 5º del Artículo 1º122 de la Ley 573 del 7 de febrero del 2000, "Mediante el cual se reviste al Presidente de la República de precisas facultades extraordinarias en aplicación del numeral 10 del Artículo 150 de la Constitución", conforma unidad normativa con el Artículo 10 de la acusada Ley 527 de 1999, dada su identidad de contenido.

---

[21] Corte Suprema de Justicia. Sala de Casación Laboral. M.P. José Roberto Herrera Vergara. Auto del 3 de diciembre de 1999. Radicación 13015. Disponible en http://www.superfinanciera.gov.co/Normativa/Jurisprudencia2000/mensajedatos049.htm. Barranquilla, Agosto 26 de 2010. 10:20 a.m.

Manifiesta la Corte Constitucional que atendiendo de que se denota el fenómeno jurídico de unidad de materia entre el Artículo 10 de la Ley 527 de 1999 acusado y el Artículo 4 del Decreto 266 del 2000 “Por el cual se dictan normas para suprimir y reformar las regulaciones, trámites y procedimientos”, dictado Con base en las facultades extraordinarias establecidas en la Ley 573 del 2000, pues regulan un mismo aspecto, esto es, el valor probatorio de los mensajes electrónicos, la Corte estima que la declaratoria de constitucionalidad comprenderá también al Artículo 4 del Decreto 266 del 2000 por las razones atrás referidas.

Se tiene igualmente que la sentencia C-831 de 2001, es relevante en la materia de estudio, que se presenta de esta forma:

El señor Daniel Peña Valenzuela en acción de inconstitucionalidad interpuso demanda contra el Artículo Sexto de la Ley 527 de 1999 considerando que éste transgrede los Artículos 28 y 152 de la Carta Magna, al establecer que cuando cualquier norma exija que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos si la información es accesible para su posterior consulta. A su juicio, se entendería que el requisito exigido en el Artículo 28 de la Constitución Política, relacionado con mandamiento escrito para proceder a un arresto o allanamiento estaría satisfecho con un mensaje de datos en los términos del artículo atacado.

El Señor Peña Valenzuela afirma que la Ley 527 ha debido tramitarse como una ley estatutaria en la medida que ésta regula una parte esencial del Artículo 28 de la Constitución Política, toda vez que regular procedimientos y recursos para su protección, mediante los requisitos especiales.

Según Peña Valenzuela , tratándose en este caso de la regulación de un derecho fundamental consagrado en el Artículo 28 de la Constitución Política la norma ha debido ser objeto de ley estatutaria y no de una ordinaria.

Los intervinientes en el escrito de la demanda, de forma unánime, defendieron la constitucionalidad de la norma acusada, finalmente, la Corte consideró que las leyes estatutarias sobre derechos fundamentales tienen por objeto desarrollarlos y complementarlos. Esto no supone que toda regulación en la cual se toquen aspectos relativos a un derecho fundamental deba hacerse por vía de ley estatutaria. La norma atacada (Artículo Sexto de la ley 527 de 1999), ni en su finalidad ni en su contenido está dirigida a afectar el núcleo esencial del derecho a la libertad personal y la inviolabilidad del domicilio.

El actor no tiene razón cuando pretende dar a la norma el alcance de regular el Artículo 28 de la Carta, por lo que la supuesta violación del Artículo 152 no tiene no tiene fundamento al no aplicarse en este caso la reserva de la ley estatutaria a que alude el demandante.

Finalmente, para el bien del comercio y para el desarrollo de los medios de información a través de redes telemáticas, la Ley 527 salió adelante a pesar de las críticas recibidas en materia procesal.

4. ENTIDADES DE CERTIFICACIÓN Y FIRMAS DIGITALES Y CERTIFICADOS

Las Certificaciones en nuestro medio, representan el soporte necesario para generar confianza y fuerza vinculante en los actos y operaciones que no han cumplido con una formalidad que los valide, asegurando la certeza de los hechos. Esta concepción ha perdurado en el tiempo a lo largo de su existencia, concluyendo entonces en la delegación de la función fedante a las Notarías Públicas.

Las Entidades certificadoras son las entidades encargados de dar fe de los hechos y actos celebrados por medios electrónicos. La seguridad en las redes, se encuentra avalada, a través de estas instituciones, sin que sean el único medio de seguridad disponible en el mercado. El objetivo y fin primordial de dichas Entidades es generar confianza a través de un respaldo económico y jurídico. Las Entidades de Certificación están reguladas en la Parte III del CAPÍTULO II de la Ley 527 de 1999.

4.1 CONCEPTO

Las Entidades de Certificación son personas jurídicas, públicas o privadas, nacionales o extranjeras, que autorizadas por la Superintendencia de Industria y Comercio, emiten certificados digitales en relación con firmas digitales, que garantizan la fiabilidad, inalterabilidad y rastreabilidad de un mensaje de

datos, proporcionando seguridad jurídica a través de una infraestructura de clave pública.

Las entidades certificadoras deben tener autorización de la superintendencia de comercio para expedir las de su competencia. Obtenido el permiso pueden estas instituciones emitir certificaciones respecto a las firmas digitales:

a. Emitir certificados en relación con las firmas digitales.
b. Ofrecer o facilitar los servicios de creación de firmas digitales certificadas.
c. Servicios de registro y estampado cronológico en la transmisión.
d. Recepción de mensajes de datos; servicios de archivo y conservación de mensajes de datos, entre otras.

4.2 NATURALEZA JURÍDICA DE LAS ENTIDADES DE CERTIFICACIÓN

Con fundamento en la Ley Marco del comercio electrónico el legislador procedió a incorporar elementos internacionales en el derecho interno, quien expidiendo la Ley 527 de 1999.

Como primera medida, se tomaron dos posiciones, quienes defienden La ley y otra, quienes demandan la inexequibilidad de la misma y reprochan las inconsistencias de esta. Una vez agotas las discusiones debatidas en el seno de la Corte Constitucional, resulta consecuente comenzar la discusión sobre la

naturaleza jurídica de la ley.

Al análisis de la actividad de la fe pública nos remontamos al tema de los tabeliones romanos, quienes “eran personas privadas que por una especial autorización del estado habían adquirido facultad para extender y legalizar documentos sobre determinados negocios jurídicos contra el pago de derechos. Estos tabeliones no ejercían, sin embargo, ningún oficio público y sus documentos no tenían fe pública. Pero si estaban bajo inspección estatal y tenían validez, sobre todo ante autoridades y tribunales fuerza legal.

4.3 ENTIDADES DE CERTIFICACION FRENTE A LA ACTIVIDAD NOTARIAL.

La discusión centrada en la fe pública. Tiene dos posiciones por un lado están la entidades de certificadoras como fedante y por otra parte, las certificadoras que no cumplen funciones de fedatarias.

La Jurisprudencia a través de la Corte Constitucional mediante Sentencia C-662 de 2000, expuso el tema de la siguiente forma:

“[...] Son dos los reparos que generan el cuestionamiento de constitucionalidad que plantea la demandante a saber: que las entidades certificadoras, estarían dando fe pública en Colombia, cuando esta función está reservada constitucionalmente de manera exclusiva a los

notarios [...]”[22]

Ante la posición planteada por nuestra corte constitucional puede afirmarse que las certificadoras no dan fe pública, puesto que no se les ha atribuido esa función por el estado lo que no implica que no puedan ser avaladas para esos efectos en un futuro, bajo las condiciones impuestas por el legislador.

4.4 LA ACTIVIDAD DE LAS ENTIDADES DE CERTIFICACIÓN.

Las certificadoras, al tenor de lo dispuesto en Ley 527 del 1999 pueden ser personas jurídicas, nacionales o extranjeras, de carácter público o privado, con autonomía administrativa y financiera, prestadoras de un servicio público, bajo la vigilancia y control de la Superintendencia de Industria y Comercio.

El servicio público, como género, puede entenderse: como toda actividad organizada que tiende a satisfacer necesidades de interés general en forma regular y continua, de acuerdo con un régimen jurídico especial, bien que se realice por el Estado directamente o por personas privadas”.

Ahora bien, la Constitución Política de Colombia en su Artículo 365 establece:

[22] Corte Constitucional de la República de Colombia. Acción Pública de Inconstitucionalidad contra la Ley 527 de 1999.. Sentencia No.C-662. M.P. Fabio Moron Díaz. Bogotá, Junio 8 de 2000.

> *[...] Los servicios públicos son inherentes a la finalidad social del Estado. Es deber del Estado asegurar su prestación eficiente a todos los habitantes del territorio nacional. Los servicios públicos estarán sometidos al régimen jurídico que fije la ley, podrán ser prestados por el Estado, directa o indirectamente, por comunidades organizadas, o por particulares. En todo caso, el Estado mantendrá la regulación, el control y la vigilancia de dichos servicios [...]*[23]

El Artículo 430 Código Sustantivo del Trabajo: define el servicio público así:

"Como servicio público toda actividad organizada que tienda a satisfacer necesidades de interés general en forma regular y continua, de acuerdo con un régimen jurídico especial, bien que se realice por el Estado, directamente o indirectamente, o por personas privadas"[24].

Ahora bien, es importante distinguir entre servicio público domiciliario y el no domiciliario. El primero está regulado por la Ley 142 de 1994, es el destinado a cubrir las necesidades básicas del ser humano. Esta ley se aplica a los servicios públicos de acueducto, alcantarillado, aseo, energía eléctrica, distribución de gas combustible, telefonía fija pública básica conmutada y la telefonía local móvil. Las entidades certificadoras atendiendo su fin primordial como es el facilitar y garantizar las transacciones comerciales por medios electrónicos y considerando que este es un servicio público, requería de forma obligada, un control, por parte de una entidad de orden estatal. Es así por lo que desde su génesis se

[23] Constitución Política de Colombia. Capítulo V. De la finalidad de social del Estado y de los servicios públicos. Art. 365. Ed. Momo Edic. Bogotá. 2005. p. 56

[24] SERNA VELÁSQUEZ, Sandra Victoria. El papel del Estado Colombiano en la provisión de bienes y servicios. Comercio Interncional. Disponible en http://www.gestiopolis.com/recursos/documentos/fulldocs/eco/edocolbsss.htm

consideró que la Superintendencia de Industria y Comercio, era el órgano idóneo para ejercer el control y la vigilancia sobre dichas entidades.

4.5 CLASES DE ENTIDADES DE CERTIFICACIÓN.

La Ley 527 de 1999 señala quienes pueden actuar como certificadoras, expresando la posibilidad de que éstas puedan ser públicas o privadas:

1. Públicas o privadas: Las Entidades de Certificación podrán ser personas jurídicas privadas o públicas, dependiendo del origen del capital con que sean constituidas.

2. Nacionales o Extranjeras: El legislador contempló la posibilidad de entidades de certificación extranjeras, teniendo en cuenta la globalización que circunda la Ley. Lo importante es que se reúnan los requisitos exigidos por la ley. En la práctica, para que los efectos jurídicos de la certificación extranjera estén ajustados a la ley colombiana, es necesario el cumplimiento de las obligaciones de inscripción para sociedades extranjeras.

3. Cámaras de Comercio: Las cámaras de comercio de acuerdo con el Decreto Reglamentario 1520 de 1978 sólo pueden ejercer las funciones señaladas en el Artículo 86 del Código de Comercio, lo que les impide competir con las actividades propias del sector privado. Esto genera un

inconveniente normativo en el sentido que las Cámaras de Comercio estarían impedidas para realizar la actividad de certificación a que se refiere la Ley 527 de 1999, sin embargo, por virtud de ésta Ley fueron expresamente facultadas.

Otra interpretación al respecto sería la siguiente: La Ley 527 de 1999, faculto a las Cámaras para ejercer la función Certificadora, de acuerdo con el Numeral 12 del Artículo 86 del Código de Comercio: "Las demás que les atribuyan las leyes y el Gobierno Nacional", se estaría dotando con una nueva función a las Cámaras de Comercio.

4. Notarios y Cónsules: De acuerdo con la Ley 527 de 1999 los notarios y los cónsules no estaban previstos como entidades de certificación. A raíz de su no inclusión, se suscitaron una serie de confusiones que encontraron respuesta en la Ley 588 de julio 5 de 2000, que las facultó para ser Entidades de Certificación, previa autorización de la Superintendencia de Industria y Comercio.

5. Entidades de Certificación Abiertas y Cerradas: El Decreto Reglamentario 1747 de 2000 en desarrollo de lo previsto por la Ley 527 de 1999 (Capítulo II), clasificó las Entidades de Certificación de la siguiente manera:

Entidades de Certificación Cerrada: Ofrece servicios propios de certificación sólo para el intercambio de mensajes entre la entidad y el suscriptor, sin exigir remuneración por ello.

La entidad de certificación cerrada es aquella que certifica el intercambio de mensajes de datos entre la entidad y el suscriptor, con la particular característica de que su servicio es gratuito.

Para su funcionamiento necesita la autorización de la Superintendencia de Industria y Comercio. Para obtener dicha autorización es necesario el cumplimiento de los siguientes requisitos:

1. Cumplir las condiciones establecidas en el artículo 29 de la Ley 527 de 1999, esto es:

a. Ser persona jurídica públicas o privadas, de origen nacional o extranjero, y las Cámaras de Comercio;
b. Contar con la capacidad económica y financiera suficiente para prestar los servicios autorizados como entidad de certificación.
c. Contar con la capacidad y elementos técnicos necesarios para la generación de firmas digitales, la emisión de certificados sobre la autenticidad de las mismas y la conservación de mensajes de datos en los términos establecidos en esta ley.

2. Que los administradores y representantes legales no estén incursos en las causales de inhabilidad previstas en el literal c) del artículo 29 de la ley 527 de 1999;

3. Estar en capacidad de cumplir los estándares mínimos que fije la Superintendencia de Industria y Comercio de acuerdo a los servicios ofrecidos.

4. Frente a la emisión de certificados, se deberá indicar expresamente que sólo podrán ser usados entre la entidad emisora y el suscriptor. Las entidades deberán informar al suscriptor de manera clara y expresa, previa expedición de los certificados, que éstos no cumplen los requisitos del artículo 15 del Decreto 1747 de 2000.

4.6 LAS ENTIDADES DE CERTIFICACIÓN, SUS FUNCIONES DEBERES Y RESPONSABILIDADES

La actividad de las entidades de certificación, como se mencionó, es la prestación de un servicio público, y como tal, su responsabilidad se extiende a la de un hombre de negocios respecto a la ejecución de su actividad, de modo tal, que cualquier incumplimiento y/ o daño que se cause como consecuencia directa o indirecta de su actividad debe ser resarcido de acuerdo con las normas sobre responsabilidad civil contractual y extracontractual.

La actividad certificadora debe ser desarrollada dentro de un marco de garantías y responsabilidad altísimas, a tal punto, que las fallas humanas o técnicas en el servicio son responsabilidad de la entidad como ente prestador de un servicio público.

Las llamadas cláusulas de exoneración de responsabilidad no son validas cuando se contrata con una entidad de certificación para la emisión de certificados digitales; los daños que se causen en una operación de comercio mediante medios electrónicos que se respalde a través de una certificadora están garantizados. La Entidad debe escoger una de las garantías que impone el Decreto 1747 de 2000.

Precisamente, las garantías del Decreto 1747, deben suplir los requerimientos económicos en la eventualidad de una indemnización de un perjuicio, por lo que no es viable jurídicamente, establecer cláusulas que exoneren a la certificadora de responsabilidad por los daños en cumplimiento de sus servicio.

La responsabilidad de la entidad es contractual y se regulará por las normas del código civil y por las normas propias del negocio celebrado, sin perjuicio de la aplicación de las normas propias sobre comercio electrónico y la aplicación de la teoría del riesgo.

Por todo lo antes mencionado es relevante señalar que proceden para las certificadoras, como mecanismos eximentes de culpa, probar diligencia y cuidado en el manejo de las herramientas de seguridad.

Las funciones de las Entidades de Certificación han sido definidas por el legislador y jurisprudencialmente. La Corte Constitucional en Sentencia C-662 de

2000, al respecto manifestó:

> *El servicio de certificación a cargo de las entidades certificadoras propende por proporcionar seguridad jurídica a las transacciones comerciales por vía informática, actuando la entidad de certificación como tercero de absoluta confianza, para lo cual la ley le atribuye importantes prerrogativas de certificación técnica, entendiendo por tal, la que versa, no sobre el contenido mismo del mensaje de datos, sino sobre las características técnicas en las que este fue emitido y sobre la comprobación de la identidad, tanto de la persona que lo ha generado, como la de quien lo ha recibido*[25].

La función principal de las certificadoras es la expedición de certificados digitales, de acuerdo con lo establecido el manual de Prácticas de Certificación, otorgando, confiabilidad y protección, debido uso de la información y conservación de los mensajes de datos en archivos digitales del sistema, permitiendo que el usuario o suscriptor tenga acceso permanente al sistema y pronta resolución de sus inquietudes y quejas, bajo la permanente realización de auditorías e inspección y vigilancia por parte de la Superintendencia de Industria y Comercio.

Por su parte el Artículo 13 del Decreto 1741 de 2000 complementa el Artículo 32 en los siguientes aspectos, para la expedición de certificados la entidad de certificación debe cumplir una tarea muy importante que en diferentes países como España, Estados Unidos o Inglaterra, la cumple la denominada “Autoridad

[25] Corte Constitucional de la República de Colombia. Sentencia de Constitucionalidad nº 662/00 de Corte Constitucional, de 08 Junio 2000 . Sentencia C-662-10 MP. Fabio Morón Díaz. Bogotá, Junio 8 de 2000.

de Registro".

En Colombia es una función y deber propio de las Entidades de Certificación, lo cual consiste en ratificar la identidad del usuario, comprobando que sea un sujeto de derecho calificado para la realización de transacciones electrónicas. Así mismo, la entidad debe tener a disposición de sus clientes la Declaración de Prácticas de Certificación, debiendo explicar de la forma más clara posible, el tipo de certificado que se está expidiendo, su grado de confiabilidad y la responsabilidad de la entidad en caso de perjuicios derivados de dicha certificación.

Como complemento, se impone la necesidad de disponer de una línea exclusiva de atención al cliente y la obligación de informar sobre la revocación de los certificados o la suspensión del servicio.

Es imperativa la conservación de la documentación que soporta las certificaciones proferidas. La Ley 527 de 1999 impone la obligación de mantener los documentos del comerciante en cualquier medio que asegure su fiel reproducción, sin establecer requisitos adicionales, así podría pensarse que los paquetes de datos a que se refiere la Ley 527 de 1999, no deben cumplir con la exigencia establecida en el Artículo 60 del Código de Comercio.

Las entidades de certificación, deben conservar el uso exclusivo de las claves

privadas, implementando las seguridades necesarias que garanticen su privacidad.

4.7 QUE SON LOS CERTIFICADOS DIGITALES

El sistema PKI tiene su apoyo fundamental en la fiabilidad y, esta sólo la puede proporcionar un tercero neutral frente a las partes (emisor y receptor del mensaje).

Los certificados digitales son emitidos, gestionados, administrados y revocados por las Autoridades de Certificación.

El certificado digital cumple dos funciones básicas:

- Garantiza que la transacción sea segura, proporcionando confiabilidad, integridad, autenticidad y no repudio.

- Permite que el receptor del mensaje de datos pueda acceder a la clave pública del remitente, para poder desencriptar el mensaje.

Los elementos básicos de un Certificado de acuerdo con el Dr. Andrés Font, son los siguientes:

- Identidad del usuario;
- Número de serie del certificado;
- Fecha de expiración del certificado;
- Copia de la clave pública del usuario;
- Identidad de la Entidad de Certificación

Es importante resaltar que no todos los mensajes de datos firmados digitalmente son certificados digitales, para tener la calidad de certificado digital debe cumplirse con los requisitos mínimos de contenido y seguridad, así como garantizar la confidencialidad, autenticación, integridad y no rechazo.

4.7.1 Certicamara. La actividad de expedir certificados en nuestro país, es hoy en día bastante limitada, sin embargo, a pesar del desconocimiento del tema, se han adelantado diversos proyectos, impulsados por la necesidad de implementar mecanismos de seguridad que agilicen los trámites y que generen una mejor calidad de vida.

Como se ha venido mencionando, sólo existe una Entidad de Certificación, abierta, autorizada por la Superintendencia de Industria y Comercio para expedir Certificados Digitales. A continuación se explica su funcionamiento y sus servicios, para entender así, en la práctica, cómo hacer uso de este servicio.

Certicamara, es la Entidad de Certificación abierta en funcionamiento, pertenece

como su nombre lo sugiere a las Cámaras de Comercio del país, ofrece tres tipos de certificados:

• Certificados de Representación;
• De pertenencia
• Certificados de Servidor Seguro.

Certificados de Representación de Empresa: son certificaciones digitales que designan una clave con una persona, indicando que ese usuario tiene la calidad de representante legal de una persona jurídica determinada al momento de expedición del certificado, siendo responsable la entidad de informar oportunamente sobre la revocación del mismo. El representante legal tendrá bajo su custodia la clave privada. De forma tal que, cuando el representante legal quiera otorgar poderes, celebrar contratos, votar en una asamblea etc., y se encuentre fuera de su domicilio, bien sea dentro del mismo país o fuera de él, podrá firmar digitalmente el documento que se requiera, el cual quedará avalado con su firma digital y tendrá, plena validez jurídica.

Certificados de Pertenencia a Empresa: Son certificaciones que designan un clave a una persona natural, señalando que ostenta un cargo determinado en una empresa. Su funcionamiento es igual al anterior. Este tipo de certificados es ideal para empresas multinacionales o nacionales con varias sedes en el país. Se ahorrará tiempo y costos de traslado, entre muchos otros

beneficios.

Certificados de Servidor Seguro: Son certificaciones que designan un clave a una dirección URL, indicando que una persona determinada tiene el control y el derecho a ser asociado a dicha dirección. Su funcionamiento es igual a los dos anteriores certificados.

Es destacable que una Entidad de Certificación al hacer parte de una Cámara de Comercio, como es el caso de Certicamara, suple las funciones de registro y de control de idoneidad de los usuarios con un elemento de confianza adicional, por su especial connotación dentro del gremio.

Ahora bien, para acceder a estos servicios de certificación digital, es necesario estar inscrito en cualquiera de las Cámaras de Comercio a nivel Nacional.

Para obtener una certificación digital se debe llenar una solicitud, que puede obtenerse en cualquiera de las Cámaras del país, la cual es necesario anexar los documentos de identificación pertinentes.

Es muy importante el reconocimiento físico de la persona que solicita la expedición del certificado digital, para lo cual debe acudir a la cámara de comercio donde se encuentra ubicado su domicilio social.

Una vez verificados los documentos presentados, Certicámara emite un certificado digital, se almacena en una tarjeta inteligente la identidad del usuario, y su capacidad de firma. Sólo el propietario del certificado digital puede hacer uso de él al introducir su número de identificación personal, similar a la clave de una tarjeta débito. Todos los clientes reciben un kit de instalación, el cual contiene un lector y una tarjeta inteligente para que pueda firmarse digitalmente el documento que se quiera proteger. Los Certificados que expide Certicamara tienen una vigencia de un año, al cabo del cual pierden su vigencia.

4.7.2 Validez de certificados extranjeros. Encontramos que de acuerdo al concepto No. 00050766, la supercomercio manifestó que sólo las Entidades Autorizadas por la Superintendencia, conforme a la ley, podrán autorizar y dar fe de las Certificaciones de Entidades extranjeras.

Se suprime el requisito, que indicaba que, para que un documento emitido en el extranjero tenga validez en Colombia, debe estar avalado por el Cónsul del país de creación y ratificado por el Ministerio de Relaciones Exteriores.

La Superintendencia de Industria y Comercio emite un listado de las Entidades de Certificación de nivel mundial, consideradas idóneas para su ejercicio en Colombia, cuya gestión y emisión de certificados es válido por el hecho de estar admitida y reconocida por la Superintendencia de Industria

y Comercio. De esta forma, la Superintendencia de Industria y Comercio tiene un mayor control y establece lasos comerciales de intermediación importantes para el futuro, en cuanto se refiere al comercio electrónico por Internet.

En la actualidad, las Entidades Financieras y Aseguradoras, poseen certificados emitidos por Compañías extranjeras, en particular el certificado que emite Verising, sin embargo, Certicámara no ha entablado acuerdos de certificación recíproca con ninguna entidad de certificación digital del exterior. Esto por cuanto la ley requiere que las entidades de certificación acreditadas en el exterior cumplan requisitos equivalentes a los exigidos a las locales. La normatividad colombiana es mucho más estricta que la de otros países, como por ejemplo, E.U., donde el proceso de identificación y emisión de los certificados digitales es libre y por tanto no obedece a los estándares de seguridad requeridos en Colombia. En este orden de ideas, puede afirmarse que jurídicamente, es función de la Superintendencia de Industria y Comercio es pronunciarse frente al particular y someter a las compañías extranjeras para que adopten certificados válidos y con respaldo jurídico en la ley colombiana.

4.8 QUE SON LAS FIRMAS DIGITALES

El concepto de firma digital ha sido asimilado como un símbolo que identifica a una persona jurídica, o natural con la cual se identifica y manifiesta su

voluntad en una acto de comercio, o jurídico en general, esta identificación digital no se aleja del concepto básico de firma, pero si es una especie particular con características propias, a través de la firma digital se pretende garantizar que un determinado mensaje de datos procede de una persona determinada; que el mensaje no ha sido modificado desde su creación y transmisión y, que el receptor no puede modificar el mensaje recibido.

La Ley 527 reconoció además, la equivalencia entre la firma manuscrita y la firma digital. Para tal efecto la firma digital debe cumplir con ciertos requisitos que expone el Artículo 28:

> *Artículo 28. Atributos de una firma digital. Cuando una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo.*
>
> *PARAGRAFO: El uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquella incorpora los siguientes atributos:*
>
> 1. *Es única a la persona que la usa.*
> 2. *Es susceptible de ser verificada.*
> 3. *Está bajo el control exclusivo de la persona que la usa.*
> 4. *Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma digital es invalidada.*
> 5 *Está conforme a las reglamentaciones adoptadas por el Gobierno*[26]*.*

Es importante en este punto, hacer la siguiente diferenciación entre los conceptos de firma electrónica, firma digital y firma certificada. La firma electrónica es aquella cuya creación implica el uso de medios informáticos, independientemente de cual

[26] Superintendencia de Industria y Comercio. Radicación 01057688. Disponible: http://www.sic.gov.co/index.php?idcategoria=7752. Barranquilla, Agosto 26 de 2010.

sea éste, es decir, que cualquier firma que implique el uso de la informática puede considerarse como firma electrónica; así la firma digital y la firma certificada son firmas electrónicas, aquella es la especie y esta es el género. Por su parte, la firma certificada es aquella que además de utilizar el proceso de clave pública es avalada por un tercero de confianza – Entidad de Certificación – por medio de la expedición de un Certificado Digital -.

Una de las formas de dar seguridad a una firma digital es mediante la encriptación, rama de las matemáticas ocupada de transformar, mensajes o datos a una apariencia inentendible y posteriormente traducirlo a un mensaje coherente.

4.8.1 Como se crea una firma digital. La firma digital se obtiene a través de un mecanismo de creación de claves denominado hash. Éste es una función de encriptación que se corre sobre un texto y lo disminuye a un tamaño estándar.

El mensaje simplificado es conocido como resumen del mensaje. Una vez el es tratado se codifica o encripta con la clave pública en los sistemas o con la clave privada en los sistemas. El producto final de esta operación es la “firma digital”.

Ejemplo de una firma digital:

> HQpumvbmbvq4ebyweonç’m7c8oñ4rjxg68vwrQ38BW65SVKN54
> LKNA4Smámis,+ò.hsp`riomsñç5ark´mspgj4lgKglgÑSLjkg465hdsh
> 54A.

Cuando el receptor recibe el mensaje encriptado utiliza su clave privada o pública para desencriptarlo, la clave contiene la misma función hash con que se encriptó el mensaje, y lo convierte en el message digest inicial, el cual debe ser idéntico al generado por el suscriptor, caso en el cual hay plena garantía de que el mensaje no ha sido alterado ni modificado.

4.8.2 Características de las firmas digitales.

1. Son únicas
2. Están bajo el control exclusivo del emisor y receptor, aunque en el sistema de clave pública una de las claves es de acceso público y puede ser conocida por cualquier persona;
3. Cada transacción que se realice debe utilizar una clave nueva, creada para un único mensaje de datos;
4. Son susceptibles de ser verificadas por la entidad de certificación que las creó;
5. Van adjuntas al documento de forma tal que pueda verificarse si el mensaje ha sido alterado después de ser encriptado;
6. Para que tengan garantía legal deben ser creadas por entidades autorizadas para tal fin.

5. LOS MEDIOS DE PAGO Y PROCEDIMIENTOS DE CERTIFICACIÓN

Las tarjetas de pago tienen diversas funciones como lo expresa la Dra. Gómez Mendoza:

> *Instrumento o medio de pago; instrumento de crédito; instrumento de garantía y como medio para obtener dinero, bien en oficinas bancarias, bien en cajeros. Como medio de pago, las tarjetas permiten el pago, de bienes y servicios sin necesidad de desembolsar dinero efectivo. Esta es la función básica y la que autoriza a denominar a todas las tarjetas como tarjetas de pago*[27]*.*

Mientras que se presenten formas de pago seguros a precios moderados y de aceptación internacional, el futuro del comercio electrónico será prominente.

Respecto a los medios de pago, se presentan dos grandes problemas; la verificación de la autenticidad y, la interceptación de claves. Los mecanismos de seguridad implementados por los establecimientos de comercio y por las entidades financieras no garantizan la autenticidad del mensaje de datos, es decir, es incierto si quien está comprando a través de la tarjeta de crédito es el verdadero titular o un delincuente. La razón principal, como se ha reiterado a lo largo del presente estudio, es el sistema de seguridad, como por ejemplo el protocolo SSL, que si bien es un mecanismo óptimo para ciertos entornos comerciales, no lo es cuando a manejo de fondos se refiere.

[27] GÓMEZ MENDOZA, María. Consideraciones Generales en torno a la Tarjeta de Crédito. Estudios en Homenaje a Joaquín Garriges. Madrid: 1971. Tomo II. p. 393

En la actualidad cuando la Entidad emisora del medio de pago confirma que los datos suministrados, son los asignados, autoriza la transacción eximiéndose de todo tipo de responsabilidad con fundamento en que de acuerdo con el Reglamento de Uso del medio de pago, las claves secretas son privadas y de uso exclusivo del titular, así, cualquier fraude que se ocasione será asumido por el titular del producto. Es evidente, entonces, que las Entidades Financieras están desconociendo que la falla, en la mayoría de los casos, se presenta en su sistema de seguridad y no por el mal manejo de las claves asignadas al cliente.

En Colombia, las autorizaciones para transacciones electrónicas por Internet no están reguladas y no existen mecanismos confiables de verificación que le permita al usuario comprador, ni al usuario vendedor, tener la plena certeza de que las transacciones que realizan son completamente seguras y respaldadas.

Sin perjuicio de los convenios, que celebran las entidades dueñas de los medios de pago con sus compradores, encontramos que la responsabilidad recae en estos últimos, la autorización - como uno de los elementos de más trascendencia en la transacción - en todos los casos, proviene del Banco emisor, lo que compromete la responsabilidad del Banco frente a la autorización, es decir, que si se presenta algún tipo de perjuicio, como consecuencia de la autorización emitida por el Banco, éste no se puede eximir de su responsabilidad y deberá responder por su acción u omisión según sea el caso.

Existen diversos medios de pago en el mercado, y las compañías emisoras de éstos, como aquellas que buscan ampliar su campo de acción, buscan, constantemente, opciones seguras de pago. De este modo, la estrategia se debe centrar en el desarrollo de medios de pago seguros, como cimiento de las transacciones por medios telemáticos. Así, quien desarrolle medios de pago seguro, de fácil acceso y a costes accesibles, tendrá el mercado en sus manos.

5.1 GÉNESIS DE LAS TARJETAS DE CRÉDITO

El sistema de intercambio o trueque de mercancías impulsó al hombre a solicitar crédito para sus actividades agrícolas a otras personas, quienes por lo general eran representantes de la iglesia. El hecho descrito constituye un caso clásico de intermediación financiera que ilustra claramente el proceso de captación de recursos monetarios.[28]

La historia de la tarjeta de crédito se remonta a finales del siglo XIX dentro de la industria hotelera con posterioridad la historia continua con las llamadas "cartas de prestigio" que emitieron las compañías petroleras Esso y Texaco hacia 1920, luego, más tarde hacia el año 1936, las tarjetas de pago para servicios aéreos.

La historia de las tarjetas de crédito se remonta a una noche de 1949, en la cual Frank Mcnamara avergonzado por no tener como pagar la cuenta del restaurante,

[28] http://www.gestiopolis.com/recursos/documentos/fulldocs/fin/tarjecredito.htm.

se le ocurrió la idea de crear una tarjeta parecida a la de los grandes almacenes, para pagar las cuentas de los restaurantes. De ahí surgió Diners Club.

El auge de la tarjeta de crédito se inicia con la aparición de la tarjeta Diners Club, y en el año de 1958 la tarjeta “American Express”, en el año 1959 el Bank of América lanza al mercado la Bank Americard con más de 3.000 bancos afiliados, la que hoy se conoce como la reconocida marca Visa International, aparece en la misma época la tarjeta “California Bank Card” que hoy en día es la marca Master Card.

La gran depresión norteamericana en los años treinta, provoco un estancamiento en las tarjetas de pago debido a la cartera morosa que se incrementó a niveles insostenibles. Hacia mediados delos años treinta varias compañías se unieron crearon la tarjeta de crédito Bell.

Hacia el año 1948, la tarjeta de crédito Diners Club se posiciono en el mercado mundial, aparece la tarjeta de American Express a finales de los años sesenta. Para la década de los años 60 los bancos crearon asociaciones con el fin de colocar un gran número de tarjetas, de donde salió la tarjeta Master Card en los años 80. A comienzo de los noventas estaban en circulación alrededor de unas 2 67 millones de tarjetas de Visa

5.2 PRINCIPALES MECANISMOS DE SEGURIDAD SSL Y SET

El SSL (Secure Sockets Layer), es el estándar desarrollado por Netscape Communications Corporation, que utiliza tecnología de encriptación para las comunicaciones entre los servidores y los navegadores. Este sistema proporciona un canal seguro para la transmisión de los detalles de la tarjeta.

Para su utilización es necesario que el usuario comprador tenga instalado un programa que le permita seleccionar el algoritmo de encriptación de sus datos personales, así como escoger la magnitud de las claves, esto es, que tamaño va a tener la firma digital que se utilizará durante la transacción. Como se sabe, la instalación del programa no es ningún problema en la medida que la página web del vendedor le permite al comprador descargar el programa sin costo. Así finalmente, las transacciones a través SSL solo se necesita llenar un formulario, cuyos datos son encriptados. El receptor al recibir los datos los desencripta y hace efectiva la transacción.

El SSL proporciona una seguridad razonable pero no lleva a ningún tramite de autenticación por la cual se le denomina a esta situación de “tarjeta no presentada”.

Así mismo, este tipo de transacciones implica un riego adicional, tanto para el

usuario vendedor, en la medida en que se haga una utilización fraudulenta de la tarjeta de crédito, como para el usuario comprador.

Por su parte el SET (Secure Electronic Transaction), desarrollado por Visa y Master Card, proporciona seguridad entre el emisor de una tarjeta de crédito el usuario y los bancos involucrados.

A diferencia del SSL el SET utiliza la encriptación para ocultar información personal de los usuarios, evitando de esta manera el uso fraudulento de éstos, generalmente empleados con fines publicitarios sin la autorización del usuario.

CONCLUSIONES

El avance de la tecnología en este nuevo milenio propone grandes retos respecto a la globalización de las relaciones nación a nación y persona a persona

Como se ha revisado en diferentes apartes a lo largo del presente trabajo es realmente necesario en nuestro país la revaluación de la realidad con que se enfrenta una economía de mercado plagada de elementos tecnológicos que no han sido incorporados a nuestro ordenamiento jurídico, o si bien se presentan normas aisladas, están no llenan los vacíos normativos que nos limitan aún más frente a los países desarrollados en términos de estructuración del comercio en línea.

El nuevo modelo económico global de comercio, que inicialmente requería establecer mecanismos de protección ante la incontenible avalancha de bienes y servicios contenida en la internet se convierten en la gran auto limitante ante la necesidad de abrir nuestra economía al mundo y hacer parte del gran supermercado mundial.

Bajo este panorama de rezago jurídico - tecnológico de nuestro país, entendiendo que nuestro marco normativo no está ajustado a la realidad, toman gran relevancia los aspecto de certificación digital, sistemas electrónicos de medio de pago y demás, que requieren toda una estructurada instrumentación de seguridad

física y legal para proporcionar seguridad, confianza y tranquilidad en los administrados, cuando estos quieran acceder al comercio electrónico, especialmente aquel que genera índices de crecimiento macroeconómicos y que impactan nuestro producto interno bruto, o sea los grandes comerciantes del país.

La evolución de los sistemas jurídicos globalizados presupone un trabajo mancomunado con los demás países del mundo, apoyándose inicialmente en los bloques económicos regionales para efectos de revisar modelos implementados y su impacto, para luego permitir una apertura consiente y bien estructurada con lineamientos, condiciones, condiciones jurídicas claras.

Es entonces conclusión clara después de adelantar este trabajo, que la unificación normativa en materia de facilitar o asegurar transacciones seguras en el comercio electrónico del país, está llamada a darse en un largo proceso de acoplamiento, donde la integración tanto interna como externa tendrán un matiz armonizador con una realidad mundial que nos empuja a una carrera contrarreloj ante el vertiginoso ritmo de crecimiento del internet y sus actores de libre mercado.

BIBLIOGRAFÍA

ANGARITA, Remolina Nelson. Internet Comercio Electrónico & Telecomuniciones. Desmaterialización, Documento y Centrales de Registro. Bogotá: Editorial Legis S.A. 2002.

CARBONEL. PINATEL, José Carlos. La Protección del Consumidor Titular de Tarjetas de Pago en la Comunidad Europea. Madrid: Ediciones Beramar, S.L. EUROLEX. 1994.

CARNELUTTI, Francisco. La Prueba Civil. Buenos Aires. Citado por RODRÍGUEZ, Gustavo Humberto. Derecho Probatorio Colombiano. Bogotá: Ediciones de Cultura latinoamericana Ltda. EDICULCO. 1979.

CUBILLOS y RINCÓN. Introducción Jurídica al Comercio Electrónica .Medellín: Ediciones Jurídicas Gustavo Ibáñez Ltda. 2002.

DIAZ GARCÍA, Alexander. Derecho Informático. Bogotá: Editorial Leyer. 2002.

ELSENPETER, Robert. VELTE, Joby. Fundamentos de Comercio Electrónico. Estados Unidos: MC Graw Hill. 2002.

FONT, Andrés. Seguridad y Certificación en el Comercio Electrónico. Aspectos

Generales y Consideraciones Estratégicas. Madrid: Fundación Retevisión. 2000.

GARCÍA RENGIFO, Ernesto. Memorias: Comercio Electrónico. Bogotá. Universidad Externado de Colombia. 2000.

MADRIÑAN DE LA TORRE, Ramón. Principios de Derecho Comercial. Séptima Edición. Bogotá: Editorial Temis S.A. 1997.

MICHELSEN, Jaramillo,Sergio. Internet Comercio Electrónico & Telecomunicaciones. Universidad de los Andes. Primera Edición. Bogotá 2002. Legis Editores S.A. 2002.

OLIVER. CUELLO, Rafael. Tributación del Comercio Electrónico. España - Valencia. Tirant Lo Blanch. 1999.

PEÑA VALENZUELA, Daniel. Aspectos Legales de Internet y del Comercio Electrónico. Bogotá: Dupre Editores Ltda. 2001.

RODÍGUEZ. TURRIAGO, Omar. Internet Comercio Electrónico & Comunicaciones. Universidad de Los Andes Facultad de Derecho. Bogotá: Editorial Legis S.A. 2002.

SARMIENTO. GARCIA, Manuel Guillermo. Responsabilidad Civil. Universidad Externado de Colombia. 2002.

TRUJILLO SÁNCHEZ, Guillermo. Internet para Abogados. Medellín Señal Editora. 2001.

WEBGRAFÍA

- http://www.aui.es/estadi/internacional/internacional.htm
- http://www.insflug.org/COMOs/conceptos-de-redes-COMO/conceptos-de-redes-COMO-2.html-info@ute.edu.ec-malito:info@ute.edu.ec
- http://es.mmxieurope.com/home.jps
- www.firmasdigitales.com
- www.onet.es
- www.certicamara.com.co
- www.crt.gov.co
- http://iblnews.com/news/noticia.php3?id=99098
- http://www.arkhaios.com/ecommerce/guia.htm
- http://www.uncitral.org/spanish/texts/electcom/ML-ELECSIGNnew.pdf
- www.setsi.mcyt.es

LEGISLACIÓN

- Decreto Reglamentario 1520 de 1978.
- Decreto 2269 de 1993.
- Decreto 2150 de 1995.
- Decreto 1122 de 1999.
- Ley 527 de 1999.
- Ley 588 de 2000.
- Ley 573 de 2000.
- Resolución 26930.
- Decreto 1747 de 2000.
- Decreto 266 de 2000.
- Constitución Política de Colombia.
- Código Penal Colombiano.
- Código de Comercio.
- Código de Procedimiento Civil.
- Código Sustantivo del Trabajo.